

# 基于区块链的 DApp 数据与行为分析

胡 腾<sup>1,2</sup> 王艳平<sup>1</sup> 张小松<sup>1</sup> 牛伟纳<sup>1</sup>

1 电子科技大学计算机科学与工程学院 成都 611731

2 中国工程物理研究院计算机应用研究所 四川 绵阳 621900

(mailhuteng@gmail.com)

**摘 要** 区块链技术近年来发展迅速,很多组织和企业开始使用基于区块链和智能合约的去中心化应用(Decentralized Applications, DApp)来增强其信息系统的功能、安全性以及扩展新业务。但由于区块链和智能合约本身可能存在安全与性能问题,因此 DApp 也会带来新的问题。为了深入研究和分析 DApp 的数据与行为现象,从而帮助用户更好地应用区块链和 DApp,首先收集了 21 类共 2 565 个 DApp,并收集了这些 DApp 从 2015 年 7 月 30 日至 2020 年 5 月 4 日(约 1 000 万区块高度)的相关数据,共包括 16302 个智能合约,7678185 个 EOA,95889930 笔外部交易和 30833719 笔内部交易;然后从数量、时间、类型以及智能合约这 4 个角度对 DApp 分布进行了深入分析,从中总结出了一些发现,这些发现可以为 DApp 开发者与区块链研究者提供有价值的参考。

**关键词:** 区块链;以太坊;DApp;数据分析;实证研究

**中图法分类号** TP309.2

## Data and Behavior Analysis of Blockchain-based DApp

HU Teng<sup>1,2</sup>, WANG Yan-ping<sup>1</sup>, ZHANG Xiao-song<sup>1</sup> and NIU Wei-na<sup>1</sup>

1 School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

2 Institute of Computer Application, China Academy of Engineering Physics, Mianyang, Sichuan 621900, China

**Abstract** Blockchain technology has evolved rapidly in recent years, as a result, many organizations and enterprises have started using decentralized applications (DApps) based on blockchain and smart contracts to enhance the functionality and security of their information systems, or to expand new businesses. However, DApps may also introduce new problems due to the possible security and performance issues of blockchain and smart contracts. In order to deeply study and analyze the data and behavioral phenomena of DApps so as to help users better apply blockchain and DApps, a total of 2565 DApps in 21 categories are first collected, as well as data related to these DApps from July 30, 2015 to May 4, 2020 (about 10 million block heights), including 16302 smart contracts, 7678185 EOA, 95889930 external transactions, and 30833719 internal transactions. Then the DApp distribution is deeply analyzed from four perspectives: number, time, category, and smart contract, and some findings are summarized from them, which can provide valuable references for DApp developers and blockchain researchers.

**Keywords** Blockchain, Ethereum, DApp, Data analysis, Empirical study

## 1 引言

区块链技术近年来发展迅速,已成为学术界和工业界的研究热点<sup>[1]</sup>。区块链具有去中心化的特点和持久性、匿名性、可审计性,使得匿名参与者之间的价值转移无需依赖权威的第三方<sup>[2-3]</sup>。因此,区块链技术也常被称为下一代互联网<sup>[4]</sup>,其应用场景也已经从电子货币扩展到金融、医疗、物联网、软

件工程等领域<sup>[5]</sup>。区块链技术已经有很多成功的应用,如以太坊<sup>[6]</sup>,它是第一个也是最大的支持智能合约的区块链平台,市值仅次于比特币<sup>[7]</sup>。

基于区块链的 DApp(Decentralized Applications)是指以区块链和智能合约为基础的去中心化应用(下文将用“DApp”来指代“基于区块链的 DApp”)。DApp 的主要特点是没有类似客户端/服务器模式的单一服务器或实体来控制它<sup>[8]</sup>。一

到稿日期:2021-02-22 返修日期:2021-05-29

基金项目:国家自然科学基金(U19A2066);四川省科技计划项目-重点研发项目(2020YFG0294);成都市科技项目-重点研发支撑计划-重大科技应用示范项目(2019-YF09-00048-CG)

This work was supported by the National Natural Science Foundation of China (U19A2066), Sichuan Science and Technology Plan Projects-Key Research and Development Projects (2020YFG0294) and Chengdu Science and Technology Project-Key R & D Support Program-Major Science and Technology Application Demonstration Project (2019-YF09-00048-CG).

通信作者:张小松(johnsonzxs@uestc.edu.cn)

个 DApp 一般是由一个 UI(通常是一个网站)和一个或多个智能合约组成,并使用区块链作为其数据存储和处理核心。开发者在区块链平台上部署一个或多个智能合约,并在 UI 上设计智能合约调用接口,通过调用这些智能合约来实现区块链分布式应用的各种功能<sup>[8]</sup>。DApp 具有与传统应用相同的一般属性,主要的区别是其数据和计算由区块链提供<sup>[8]</sup>。DApp 继承了区块链和智能合约的去中心化、开放性、防篡改和可追溯性等特点。因此,它可以在降低开发者成本的同时,提高其应用程序的可信度。DApp 为用户提供了一个安全、便捷的平台环境,用户可以在该平台上进行转账、分享信息、签订合同等操作。

已有很多研究者基于区块链或智能合约实现了 DApp,并将其用于增强信息系统的功能、安全性以及扩展新业务。文献[9]基于智能合约设计了一个双链信托业务底层平台,实现了对信息权限的严格控制,增强了风险管理并实现了信托业务的高数据化转型;文献[10]提出了一个基于联盟区块链的医疗健康数据安全模型,该模型将数据存储存储在区块链上,并将完整医疗数据加密存储在分布式数据库,在安全存储用户医疗健康数据的同时,提高了数据在各医疗机构间的共享效率。文献[11]提出一种基于许可链构建的新型客户服务平台技术架构,该架构整合联盟链和私有链,建立了企业与客户之间、企业各部门之间的可信数据共享链路。

但目前关于 DApp 的研究和分析尚不充分,缺乏针对 DApp 中的用户、智能合约、交易等数据的深入分析,而这些数据及其行为现象能够使我们更好地了解以太坊生态系统和 DApp 的当前状态与变化。为了更好地研究和深入了解 DApp,我们收集了 21 类共 2565 个 DApp。同时,我们还收集了这些 DApp 的相关数据,包括 16302 个智能合约、7678185 个外部账户、95889930 笔外部交易和 30833719 笔内部交易。本文基于对这些数据及行为的分析研究,阐述了基于区块链的 DApp 的应用现状与前景。

## 2 研究背景和相关工作

### 2.1 DApp

本文中的 DApp 是指基于区块链的去中心化应用程序。与传统 App 相比,其主要区别在于数据和计算由区块链提供<sup>[8]</sup>。随着以太坊等分布式账本技术的发展和普及<sup>[6]</sup>,DApp 的数量近年来也保持了快速增长,并越来越受到关注。DApp 可以通过其后端调用以任何语言编写的前端代码和用户界面。后端代码部署在区块链系统上,我们通常称之为智能合约。智能合约负责操作逻辑和数据存储,并通过交易与 DApp 前端或多个智能合约进行交互。如果 DApp 的程序逻辑和功能很简单,则它一般只包含一个智能合约。由于智能合约通常有长度限制,因此 DApp 通过包含多个智能合约来实现更复杂的功能。如今,DApp 受到了很多关注,一些 DApp 相当流行,如著名的游戏 DApp“CryptoKitties”<sup>[12]</sup>。该游戏 DApp 允许玩家繁殖、收集和出售虚拟猫。虚拟猫和游戏的所有操作都记录在区块链上,因此可以保证游戏的公平性。DApp 拥有诸多优势,但也存在一些问题,如 Crypto-

Kitties 在用户使用最高峰值时会导致以太坊网络拥塞<sup>[13]</sup>。

### 2.2 以太坊

以太坊是 2014 年提出的开源区块链平台,是迄今为止最大的支持智能合约的区块链平台<sup>[14]</sup>,并且它的市场价值仅次于最大的区块链平台比特币。以太坊及其智能合约促进了 DApp 的发展,任何开发人员都可以通过智能合约创建 DApp,然后将其部署并发布在以太坊平台上。截至撰写本文时,以太坊区块链已超 1000 万个区块高度,每个区块包含许多交易。以太坊也拥有自己的加密货币,被称为以太币(Ether)。像其他数字货币一样,Ether 也可以在用户之间进行流通。开发人员可以支付 Ether 来保持其应用程序运行,其中包括交易费和计算服务<sup>[15]</sup>。

### 2.3 账户和智能合约

账户是以太坊的基本单位<sup>[16]</sup>。每个账户都有一个唯一的地址,长度为 20 个字节。以太坊区块链中的交易实际上是账户之间信息和价值的转移<sup>[17]</sup>。以太坊中有两种类型的账户:外部账户(Externally Owned Account,EOA)和合约账户(Contract Account,CA)。

EOA:用户可以任意创建该账户,并使用私钥对其进行控制。账户的地址是 EOA 的唯一标识符。它没有可执行代码,但可以用于存储当前账户的余额或通过发送交易来转移以太币,还可以用于部署或调用智能合约。

CA:也称为智能合约。与 EOA 一样,智能合约也具有账户当前的以太币余额信息和唯一的地址,但是其地址由合约创建者的地址和创建它的交易确定。在以太坊中,智能合约的本质是由字节码组成的执行程序,当满足触发条件时可以自动执行。此外,一旦智能合约部署在区块链上,任何人(包括它的开发人员)都无法对其进行修改。

这两种账户的主要区别在于,智能合约包含可执行代码,而 EOA 不包含<sup>[16]</sup>。此外,智能合约可以通过 EOA 或其他智能合约来创建,EOA 则不能<sup>[6]</sup>。

### 2.4 交易

区块链是开源共享的交易数据库<sup>[18]</sup>。一个区块可以包含许多次交易,这些交易是从一个账户发送到另一个账户的信息。以太坊中主要数据活动都是由交易触发的,包括转移以太币、调用智能合约和创建合约等。

交易有两种类型:外部交易(external transactions)和内部交易(internal transactions)。从 EOA 发起的交易被称为外部交易<sup>[15]</sup>,而从智能合约发送到其他账户的交易被称为内部交易。区块链网络中的每个参与者都可以在区块链上同步和验证交易数据。值得注意的是,由于内部交易数据未存储在区块链的区块中,因此无法直接通过解析块获得<sup>[15]</sup>。

### 2.5 以太币和代币

以太币是以太坊的原生加密货币,可以在账户之间进行交易或转移。以太坊用户通过发送一笔交易来将以太币转移给其他人,该交易的价值字段表明被转移的以太币数量。另外,以太坊要求用户支付交易费(Gas),以保护区块链免受琐碎交易或恶意交易,从而避免资源浪费<sup>[6]</sup>。代币(Token)是由智能合约实现的一种加密货币<sup>[16]</sup>。代币也可以交易和转

移,以及和以太币进行交换。

### 3 数据收集

#### 3.1 DApp 和智能合约的信息收集

我们从 4 个 DApp 的发布网站收集信息,包括 State of the Dapps<sup>[19]</sup>, DappRadar<sup>[20]</sup>, Dapp.com<sup>[21]</sup> 和 DappReview<sup>[22]</sup>。从上述网站收集的信息主要包括 DApp 的基本信息(名称、类型、创建时间等)以及相关的合约地址。我们仅收集了以太坊平台上的 DApp,表 1 列出了收集的 DApp 和智能合约的详细信息。表中的“Count”代表所有类别的总和,“Total”表示去除重复项的 DApp 总数,这是因为某些 DApp 属于多个类别。

表 1 DApps、智能合约和 EOA 数量统计表

Table 1 Statistics of DApps, smart contracts, and EOAs

Category	# of DApps	# of Smart Contracts	# of EOAs
Game	745	3 279	699 737
HighRisk	678	967	1 262 911
Gambling	574	3 090	1 357 652
Finance	194	4 614	1 502 040
Exchange	171	3 871	1 794 878
Social	128	249	640 868
Marketplace	117	1 174	423 139
Utility	95	285	515 534
Other	82	164	24 267
Collectible	66	125	8 154
Media	54	182	257 265
Development	52	114	562 624
Wallet	31	47	814 123
Governance	25	56	241 551
Property	25	74	134 356
Security	20	32	350 596
Storage	14	15	289 627
Identity	13	21	100 380
Health	8	9	1 793
Energy	6	9	13 149
Insurance	1	4	36
Count	3 099	18 381	10 994 680
Total	2 565	16 302	7 678 185

#### 3.2 交易数据收集

我们从 2 565 个 DApp 包含的 16 302 个智能合约中收集了交易,交易一共包括 95 889 930 笔外部交易和 30 833 719 笔内部交易,范围从 2015 年 7 月 30 日(0 区块高度)到 2020 年 5 月 4 日(约 1 000 万区块高度)。由于某些 DApp 的智能合约创建时间晚于 2020 年 5 月 4 日,我们额外收集了这部分交易,所以我们的分析发现和数据图表有时显示交易时间超过了 2020 年 5 月 4 日。我们通过两种方式收集智能合约的交易,一种是通过以太坊客户端同步所有历史交易数据,使用 Parity 客户端并将其设置为跟踪模式(trace-on mode),以便它可以计算和存储跟踪数据(tracing data);另一种是使用 Etherscan<sup>[23]</sup>提供的 API 下载智能合约的交易并以 JSON 格式存储数据。尽管该 API 声称只能下载最近的 10 000 个交易,但可以通过修改块范围来获取合约的所有交易。表 2 列出了有关智能合约交易的详细信息,表中的“Count”和“Total”与表 1 中的含义相同。

表 2 外部交易和内部交易的数量统计

Table 2 Statistics of external transactions and internal transactions

Category	# of External Transactions	# of Internal Transactions
Game	21 687 738	7 595 511
HighRisk	6 888 507	4 901 120
Gambling	13 241 563	7 950 204
Finance	11 565 499	3 591 211
Exchange	35 106 097	10 359 431
Social	2 140 898	450 158
Marketplace	8 935 266	4 567 057
Utility	1 903 379	206 210
Other	195 841	34 009
Collectible	330 556	172 854
Media	1 055 239	12 663
Development	2 451 185	2 035 777
Wallet	4 165 506	54 846
Governance	1 004 910	16 252
Property	2 549 423	440 589
Security	1 376 100	350
Storage	1 581 206	12
Identity	1 806 282	432 195
Health	3 347	4
Energy	40 082	54
Insurance	189	0
Count	118 028 813	42 820 507
Total	95 889 930	30 833 719

#### 3.3 账户信息收集

除了智能合约,我们还收集了 EOA 的地址。由于每笔交易都与一个发送帐户地址和一个接收帐户地址相关联,因此我们可以通过检查交易的接收字段来识别该帐户地址。若交易的接收字段等于 Null 可判断该交易创建了一个智能合约,若交易的接收字段是一段地址,那么这个地址为一个 EOA 的地址。表 1 还列出了收集的 EOA 的详细信息。

### 4 分析结果与结论

我们对 DApp 进行多维度细致的分析,并从中发现了关于区块链的独特现象,这可以帮助我们观察 DApp 的行为,并增进我们对区块链的理解,同时利用这些发现还可以帮助研究者解决区块链上的一些问题,如 DApp 的真实使用情况如何、哪些类型的 DApp 更值得投入、哪一类 DApp 的用户多且使用频率高、DApp 什么时候开始变得“热门”起来、DApp 中智能合约的情况、是否需要在 DApp 创建时就创建所有的智能合约、DApp 中的智能合约是否只能有一个创建者等。本文首先对收集到的所有数据进行整理,数据预处理将异构数据按照各类型整理清洗出来,包括去除失败的交易数据等;然后对预处理完毕的数据进行统计分析并构建数据分布图;最后根据构建好的各类分布图进行验证与分析,并得出结论。分析流程如图 1 所示。

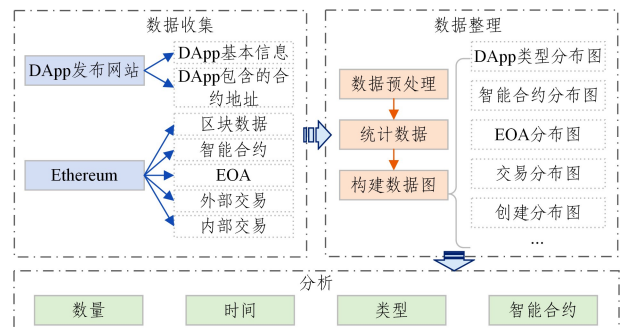


图 1 分析流程示意图

Fig. 1 Schematic diagram of analysis process

### 4.1 DApp 的数量分布

根据表 1 中收集的数据,DApp 共分为 21 个类别,其中包括 20 个已知类别,未知类别的 DApp 归为“Other”类别。一些 DApp 属于多个类别,因此所有 DApp 的数量不等于所有类别的总和。DApp 类别的分布如图 2 所示,前 3 个 DApp 类别是“Game”“HighRisk”和“Gambling”,占 DApp 总数的 64.4%,前 6 类占 DApp 总数的 80.3%,其余 15 类的总占比少于总数的 20%。其中,“HighRisk”类别需要特别提及,一些具有恶意目的的 DApp 被归类为“HighRisk”类别。经过人工检查和验证,我们发现“HighRisk”中的 DApp 有 15.6%也属于“Game”类别,有 13.9%也属于“Gambling”类别,而有 4.4%也属于“Finance”类别。这个发现与真实情况是一致的,“Game”和“Gambling”类别中存在包含不公平规则的 DApp,而“Finance”中也存在诸如庞氏骗局之类的金融欺诈 DApp。

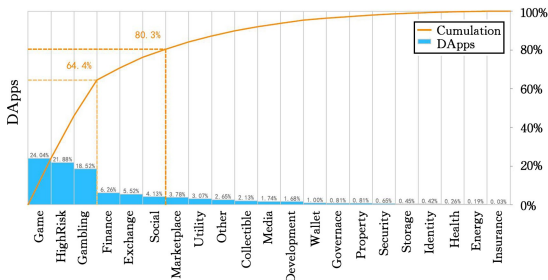


图 2 DApp 的类型分布  
Fig. 2 Distribution of DApp categories

图 3 给出了 DApp 不同类别的智能合约分布。智能合约数量排前 4 的 DApp 类别分别是“Finance”“Exchange”“Game”和“Gambling”,共占总数的 80.8%。如图 4 所示,EOA 数量最多的前 3 个 DApp 类别分别是“Exchange”“Finance”和“Gambling”,总共占总数的 42.3%,而排前 9 的 DApp 共占了 EOA 总数的 83.2%。根据表 2 中收集的数据,图 5 和图 6 分别展示了不同 DApp 类别的外部交易和内部交易分布。总的来说,包含交易数量最多的前 3 个 DApp 类别分别是“Exchange”“Game”和“Gambling”,约占总数的 60%。从图 2—图 6 可以看出:

(1)与金融相关的 DApp(“Finance”和“Exchange”)在用户中最受欢迎(拥有最多的 EOA 和交易),其次是娱乐相关的 DApp(“Game”和“Gambling”),然后是“Social”类的 DApp。但是,娱乐相关的 DApp 最受开发者的青睐(相关的 DApp 数量最多)。

(2)金融相关的 DApp 数量(“Finance”和“Exchange”)所占比例不高(6.26%和 5.52%),但它们却拥有最多的智能合约(25.1%和 21.06%)和 EOA(13.66%和 16.32%)。特别是“Exchange”类 DApp,仅占总数的 5.52%,但其包含的智能合约数量却占了总数的 21.06%(排第二),用户数量占了总数的 16.32%(EOA 数量排第一),以及其外部交易和内部交易都是所有类别中最多的。这种现象表明“Exchange”类别是使用最广泛的类别,这与区块链最热门的应用是加密货币平台有关(如比特币,以太坊),同时也表明了目前很大一部分用户将区块链作为加密货币来使用。

(3)一些新的 DApp 应用程序场景(如“Health”“Energy”和“Insurance”)在 DApp 数量、智能合约数量、用户数量、交易

数量等方面所占的比例都非常低。另一个有趣的发现是“Other”类是不属于其他 20 个类别的 DApp,占有 DApp 的 2.65%(第 9 位),但其 EOA(0.22%,第 17 位)、外部交易(0.17%,第 18 位)和内部交易(0.08%,第 14 位)所占的比例都非常低,这可能是 DApp 的开发人员正在针对新的应用场景进行一些开发测试,其产生的数据行为也是开发人员自己的测试帐号。

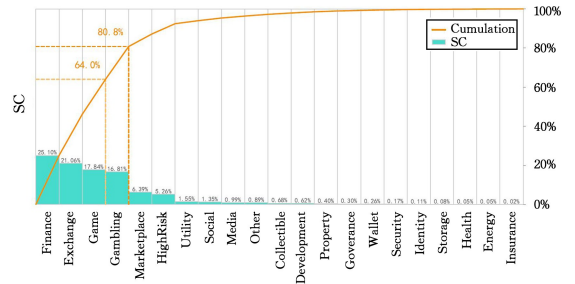


图 3 DApp 中智能合约的分布

Fig. 3 Smart contract distribution of DApp

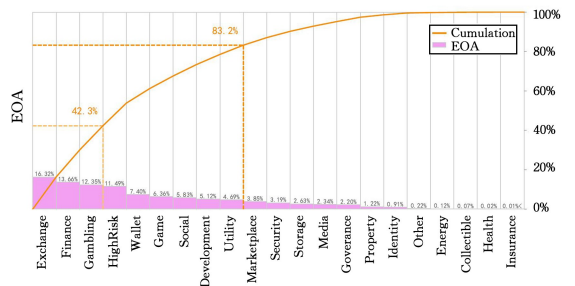


图 4 DApp 中 EOA 的分布

Fig. 4 EOA distribution of different DApp categories

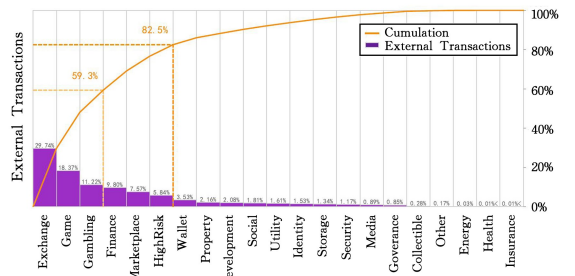


图 5 DApp 中外部交易的分布

Fig. 5 External transactions distribution of different DApp categories

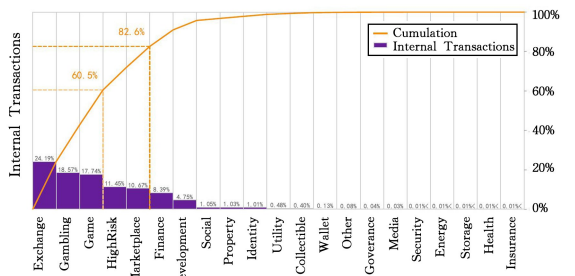


图 6 DApp 中内部交易的分布

Fig. 6 Internal transactions distribution of different DApp categories

### 4.2 DApp 的时间分布

为了更好地分析 DApp 的时间分布,我们进行了一些定

义。我们认为,在网站上发布的时间并不是 DApp 真正开始使用的时间。例如:“Golem”是“Development”类别中的一个 DApp,其在 State of the Dapps<sup>[19]</sup>的提交日期为 2015 年 4 月 23 日,它是我们收集的所有 DApp 中创建日期最早的。但是我们发现它包含的所有智能合约中,创建时间最早的智能合约<sup>1)</sup>是在 2016 年 11 月 10 日创建的,这意味着该 DApp 实际上应该在 2016 年 11 月 10 日以后才投入使用。因此,我们认为它的真实创建日期应为 2016 年 11 月 10 日。再举一个例子:“Gnosis”是一个“Exchange”类的 DApp,它在 State of the Dapps<sup>[19]</sup>上显示的提交日期为 2017 年 1 月 26 日。但我们发现其第一个智能合约<sup>2)</sup>于 2016 年 08 月 21 日创建并开始有交易产生,这意味着尽管此 DApp 于 2017 年发布,但已开始使用半年。这可能是因为在发布 DApp 之前进行了测试,这种情况我们仍然认为 DApp 的创建时间是首次使用它的时间,即 2016 年 08 月 21 日。因此,我们定义 DApp 的创建时间、终止时间和存活时间如下。

(1) 创建时间:我们将 DApp 中智能合约的创建时间用作 DApp 的创建时间。如果 DApp 具有多个合约,则将第一个合约的创建时间作为其创建时间。

(2) 终止时间:DApp 超过 3 个月未生成交易,并且此后都未产生任何交易。我们将其最后一次交易的时间作

为 DApp 的终止时间。

(3) 存活时间:一个 DApp 从创建到终止使用的天数。

图 7 给出了 DApp 创建时间的分布。图中蓝色条形表示当天创建了新 DApp,其长度表示当天创建的 DApp 数量;橙色曲线代表 DApp 的累积数量;红色曲线表示 DApp 创建数量的趋势;绿色直线代表 DApp 创建数量的平均值,其值约为每天 1.65 个。我们从图 7 中可以分析出一些现象:红色趋势线和橙色累积线显示从 2017 年 1 月开始 DApp 的数量逐渐增加,并且从 2017 年 8 月开始,每天新 DApp 的数量增长超过了平均线;从 2018 年 1 月左右开始,出现了大量新 DApp,并且趋势线和累积线出现拐点,增长趋势一直持续到 2018 年 4 月才开始出现小幅下降,在接下来的几个月中,它保持了较高的增长率,趋势几乎没有波动;从 2018 年 7 月开始出现下降趋势,直到 2018 年 7 月 18 日趋势线达到谷底,然后又开始稳步上升;2018 年 9 月 26 日为日新增 DApp 数量最多的一天(增加了 15 个 DApp);2018 年 10 月 24 日达到趋势线峰值,此后一直持续下降,直到 2019 年 2 月左右,而累积线增长趋势也减弱;从 2019 年 2 月到 2020 年 7 月,每天新增的 DApp 数量仍接近或高于平均水平,趋势线的波动较为稳定;2020 年 7 月 7 日,收集到了最后一个新增 DApp,累积线达到最大值(共 2565 个 DApp)。

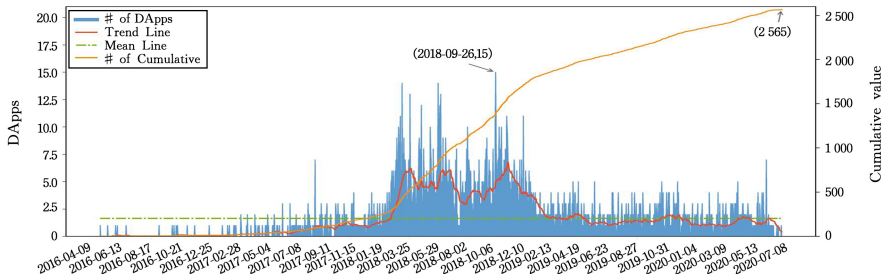


图 7 DApp 的创建时间分布(电子版为彩色)

Fig. 7 Distribution of DApp creation time

图 8 给出了 DApp 的存活数量随时间的变化。蓝色条形表示当天新创建的 DApp 数量,蓝色曲线表示 DApp 的累积数量,绿色条形表示当天终止的 DApp 数量,绿色曲线表示已终

止的 DApp 累积数量,红色曲线表示当前存活 DApp 的累积数量。根据我们收集的数据,总共创建了 2565 个 DApp,已终止了 1421 个 DApp,目前还有 1144 个 DApp 正在使用中。

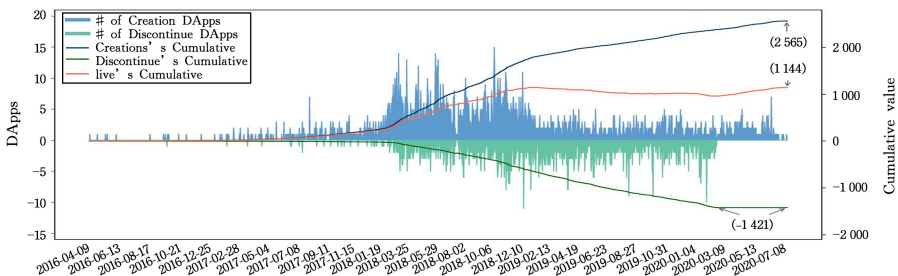


图 8 DApp 的存活数量分布(电子版为彩色)

Fig. 8 Distribution of number of living DApp

图 9 给出了所有 DApp 的存活时间情况:有 94 个 DApp (占总数的 3.66%)仅使用一天,其中一些 DApp 除了创建合约的交易信息外没有其他交易产生,造成这种情况的原因可能是 DApp 缺乏推广,未能成功吸引后续用户,也有可能是开

发人员在进行测试,测试时发现问题后放弃了该 DApp;18.01%的 DApp 的存活时间不超过 1 个月,33.06%的 DApp 的存活时间不超过一个季度,45.26%的 DApp 的存活时间不超过半年,而 63.08%的 DApp 的存活时间不超过一年;有

<sup>1)</sup> 0xa74476443119A942dE498590Fe1f2454d7D4aC0d

<sup>2)</sup> 0x5aaE5c59D642E5fD45b427Df6eD478b49d55FEfD

36.92%的 DApp 存活时间在一年以上,13.38%的 DApp 的存活时间在两年以上,只有 1.33%的 DApp(共 34 个)存活了三年以上。可以看出,DApp 的总体实际使用情况并不乐观,超过一半的 DApp 不再被用户使用。

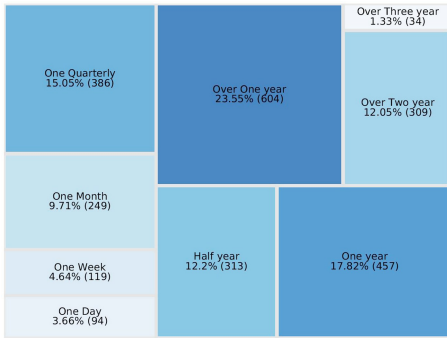
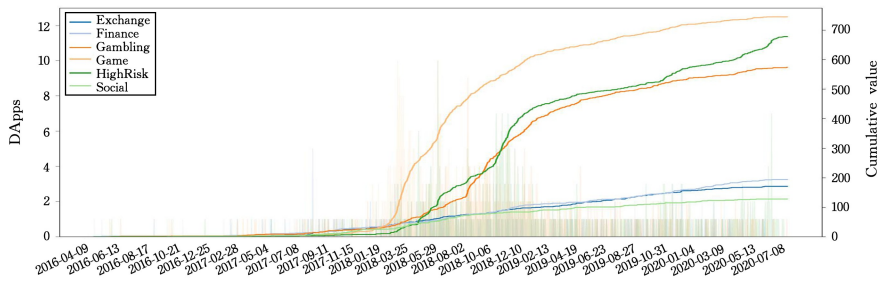


图 9 DApp 的存活时间情况  
Fig. 9 Live time of all DApps

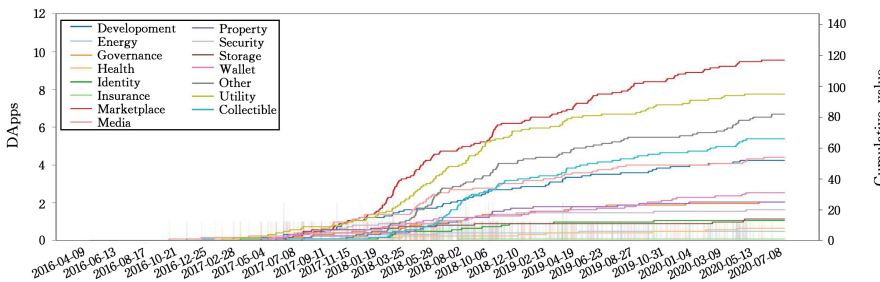
### 4.3 DApp 的类型分布

我们对 DApp 的每个类别分别进行了分析,图 10 显示了每个类别的创建时间分布。正如上文提到的,排名前 6 的类别占总数的 80%以上,如图 10(a)所示,其余 15 个类别显示在图 10(b)中。

根据我们收集的数据,表 3 为各类中第一个 DApp 的创建时间。从表 3 可知,最早创建的 DApp 类型是“Finance”(2016 年 4 月 9 日),其次是“Gambling”类以及“HighRisk”类 DApp。首个“Exchange”“Social”“Game”“Media”和“Development”类 DApp 均于 2016 年创建。除了“Insurance”之外,其他 12 个类别也于 2017 年上半年开始创建。“Insurance”是所有类别中最晚创建的类别,也是数量最少的类别。从图 10 中还可以看出,尽管每个类别的第一个 DApp 创建的时间都比较早,但它们在 2018 年 1 月之后才开始大量出现,我们认为这与区块链技术的普及有关。



(a) The top 6 DApp categories



(b) The remaining 15 DApp categories

图 10 DApp 每类的创建时间分布

Fig. 10 Creation time distribution of each category of DApp

表 3 各类别中第一个 DApp 的创建时间

Table 3 Creation time of the first DApp in each category

Category	Creation Time of first DApp
Game	2016/9/24
HighRisk	2016/5/18
Gambling	2016/5/14
Finance	2016/4/9
Exchange	2016/8/21
Social	2016/9/20
Marketplace	2017/5/29
Utility	2017/1/28
Other	2017/7/26
Collectible	2017/6/22
Media	2016/10/2
Development	2016/11/10
Wallet	2017/5/18
Governance	2017/4/25
Property	2017/4/26
Security	2017/5/16
Storage	2017/6/19
Identity	2017/3/10
Health	2017/1/12
Energy	2017/6/28
Insurance	2018/7/12

图 11 给出了 DApp 的存活率随类别变化情况。创建 DApp 数量排前 3 的类别为“Game”“HighRisk”和“Gambling”,它们的终止 DApp 数量也最多,即存活率分别为 36.38%,34.22%和 29.27%。除此之外,“Other”类的存活率也只有 39%,这可能是开发人员正在尝试新的应用场景,因此其后续使用率很低。就 DApp 的数量和存活的数量而言,“Finance”和“Exchange”这两个类别的排名分别为第 4 和第 5,并且存活率都超过 72%,说明这两类 DApp 已被用户广泛接受和使用。造成这种情况的原因可能仍然是区块链本身作为加密货币或代币已被公众所熟知。“Wallet”类也属于金融 DApp,虽然数量很少,但是 77.42%的存活率也证明了这一点。“Development”的存活率是 84.62%(最高),可能是因为其中的 DApp 可用于支持现有系统的应用程序,以及支持其他应用程序的开发。

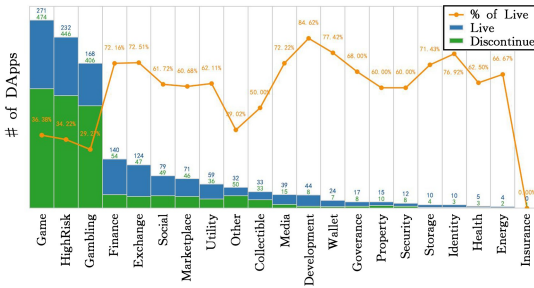


图 11 每类 DApp 的存活率

Fig. 11 Live ratio of all each category

4.4 DApp 中智能合约的分布

从图 3 可以看出,排名前 4 位的类别创建的智能合约总数的 80.8%。如“Finance”类别仅占有 DApp 的 6.26%,但其智能合约的数量却占了总数的约 1/4。

图 12 为 DApp 中智能合约的累积分布情况,大约 66% 的 DApp(1689 个)仅包含 1 个合约,超过 14% 的 DApp(364 个)仅包含 1 个或 2 个合约,少于或等于 3 个合约的 DApp 超过 86%(161 个),超过 98% 的 DApp(2515 个)包含少于 20 个合约。只有 21 个 DApp 拥有超过 50 个合约,占 0.82%;只有 9 个 DApp 拥有 100 个以上的合约,占 0.35%;只有 3 个 DApp 拥有 1000 个以上的合约,分别为 1463 个、2275 个和 3334 个。表 4 列出了智能合约数量最多的前 9 个 DApp,根据我们收集的数据,智能合约数量最多的 DApp 是“ETH-Lend”,它是一个完全去中心化的金融市场,允许来自世界各地的贷方和借款人使用区块链和智能合约以安全透明的方式创建点对点借贷协议。

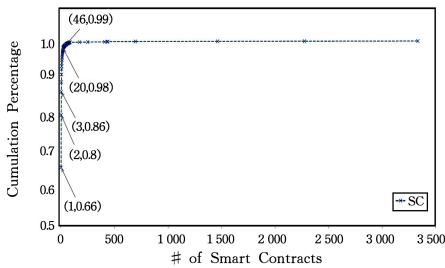


图 12 DApp 中智能合约的累积分布

Fig. 12 Cumulative distribution of smart contracts

表 4 包含智能合约最多的 9 个 DApp

Table 4 Top 9 DApps with the largest number of smart contracts

Category	DApp Name	# of Smart Contracts
Finance	ETHLend	3334
Exchange	Uniswap	2275
Gambling	Ethorse	1463
Marketplace/Exchange	Mintbase	695
Finance	NEST	438
Game	Crypto Versus	433
Exchange	Bancor	409
Gambling	0xgame	250
Game/Marketplace	Ethercraft	173

除此之外,我们发现总共有 876 个 DApp 具有不止 1 个智能合约,并具有以下一些现象:

第一,我们发现并不是所有的 DApp 都会第一时间创建

所有智能合约。有 24.4%(214 个)的 DApp 在一开始就创建了其所有的合约,并且没有增加新合约,在其余的 662 个 DApp 中,在第一时间创建的合约数量约占自身合约总数的 25.51%(平均值)。

第二,我们发现并非 DApp 中的所有智能合约都是由单个创建者创建的。有 509 个 DApp(占 58.11%)由一个创建者创建,其余 367 个 DApp(占 41.89%)由两个或更多创建者参与合约的创建。

第三,我们发现可以通过外部交易或内部交易来创建智能合约。在 93.61%(820 个)的 DApp 中,所有智能合约都是通过外部交易或内部交易单独创建的,其中 814 个合约完全由外部交易创建,只有 6 个完全由内部交易创建。在 6.39%(56 个)的 DApp 中,它们的智能合约既有由内部交易创建的,也有由外部交易创建的。

第四,我们发现一些智能合约在不同的 DApp 中有重用的现象。在包含 16516 个智能合约的 2565 个 DApp 中,重用的合约数量为 214 个,去除重用合约后数量为 16302 个,重用率为 1.31%。

**结束语** 本文介绍了区块链及 DApp 的相关背景知识,然后收集了 21 类共 2565 个 DApp 的相关信息,并从以太坊上收集了这些 DApp 的智能合约和交易数据,基于这些数据从数量、时间、类型和智能合约情况 4 个方面对 DApp 进行了深入分析,并从中总结出了一些有价值的发现。未来我们将继续深入研究 DApp 中数据行为的内在联系,并研究如何自动化地检测与识别有恶意行为的 DApp。

参考文献

- [1] SWAN M. Blockchain:Blueprint for a new economy [M]. O'Reilly Media, Inc., 2015.
- [2] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: A survey [J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.
- [3] CHEN W, ZHENG Z, CUI J, et al. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology [C] // Proceedings of the 2018 World Wide Web Conference. 2018: 1409-1418.
- [4] FERNANDEZ-CARAMES T M, FRAGA-LAMAS P. A review on the application of blockchain to the next generation of cyber-secure industry 4.0 smart factories [J]. IEEE Access, 2019, 7: 45201-45218.
- [5] LI X, JIANG P, CHEN T, et al. A survey on the security of blockchain systems [J]. Future Generation Computer Systems, 2020, 107: 841-853.
- [6] WOOD G. Ethereum: A secure decentralised generalised transaction ledger [OL]. <https://files.gitter.im/ethereum/yellowpaper/V1yt/Paper.pdf>.
- [7] CHEN T, LI Z, ZHU Y, et al. Understanding ethereum via graph analysis [J]. ACM Transactions on Internet Technology (TOIT), 2020, 20(2): 1-32.
- [8] METCALFE W. Ethereum, Smart Contracts, DApps [M]. Block-

chain and Crypt Currency. Singapore:Springer,2020:77-93.

- [9] KE Y J,JING M H,ZHENG H Y. Application Research of Blockchain Technology in Trust Industry [J]. Computer Science,2020,47(6A):591-595.
- [10] FENG T,JIAO Y,FANG J L,et al. Medical Health Data Security Model Based on Alliance Blockchain[J]. Computer Science, 2020,47(4):305-311.
- [11] ZHANG Q M,LU J H,LI S Z,et al. Building Innovative Enterprise Customer Service Technology Platform Based on Blockchain[J]. Computer Science,2020,47(6A):639-642.
- [12] BOWLES N. Cryptokitties, explained... mostly [EB/OL]. The New York Times. 2017 Dec. [2017-12-28]. <https://www.nytimes.com/2017/12/28/style/cryptokitties-want-a-blockchain-snu-ggle.html>.
- [13] TEPPER F. People have spent over \$1 M buying virtual cats on the Ethereum Blockchain [EB/OL]. [2017-12-03]. <https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/>.
- [14] LI Z H. Ethereum Smart Contract Optimization and Transaction Network Security Analysis [D]. Chendu: University of Electronic Science and Technology of China,2020.
- [15] CHEN T,LI Z,ZHANG Y,et al. Dataether: Data exploration framework for ethereum[C]// 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). 2019: 1369-1380.
- [16] BUTERIN V,WOOD G,WILCKE J. Ethereum homestead documentation[OL]. <https://ethdocs.org/en/latest/index.html>.
- [17] BUTERIN V. A next-generation smart contract and decentralized application platform[OL]. <http://blog.lavoiedubitcoin.info/public/Bibliotheque/EthereumWhitePaper.pdf>.
- [18] Ethereum Solidity. Solidity documentation [EB/OL]. [2019]. <https://solidity.readthedocs.io/en/v0.5.11/index.html>.
- [19] State of the dapps [EB/OL]. [2020]. <https://stateofthedapps.com/>.
- [20] Dappradar [EB/OL]. [2019]. <https://dappradar.com/>.
- [21] Dapp.com [EB/OL]. [2020]. <https://dapp.com/>.
- [22] Dappreview [EB/OL]. [2020]. <https://dapp.review/>.
- [23] TEAM E. Etherscan: The ethereum block explorer [EB/OL]. [2017]. <https://etherscan.io/>.



**HU Teng**, born in 1988, Ph.D. His main research interests include cybersecurity-related issues with artificial intelligence, blockchain, and big data technologies.



**ZHANG Xiao-song**, born in 1968, Ph.D., professor. His main research interests include software vulnerability analysis, program analysis, network security, and data security.